ES

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO EUROPEO, AL COMITÉ ECONÓMICO Y SOCIAL Y AL COMITÉ DE LAS REGIONES

Seguridad de las redes y de la información: Propuesta para un enfoque político europeo

Seguridad de las redes y de la información:
Propuesta para un enfoque político europeo

Índice

1. Introducción

La seguridad de las redes electrónicas y de los sistemas de información suscita cada ve más preocupación, en paralelo al rápido aumento del número de usuarios y del valor de sus transacciones. La seguridad ha cobrado ahora una importancia crítica, hasta el punto de que constituye un requisito previo para el crecimiento del comercio electrónico y el funcionamiento de la economía en su conjunto. La combinación de varios factores explica que la seguridad de la información y de las comunicaciones se encuentre en la actualidad a la cabeza de las prioridades políticas de la Unión Europea:

- Las administraciones públicas se han dado cuenta de hasta qué punto la economía y los ciudadanos dependen del funcionamiento eficaz de las redes de comunicación y varias de ellas han comenzado a revisar sus disposiciones en materia de seguridad.

- Internet ha creado una conectividad mundial que pone en contacto millones de redes, grandes y pequeñas, y cientos de millones de ordenadores individuales y, cada vez más, otros aparatos como los teléfonos móviles. Ello ha llevado consigo una reducción considerable del coste del acceso ilegal y a distancia a valiosa información económica.

- Es bien conocida la difusión a través de Internet de virus que han causado importantes daños por destrucción de información o denegación de acceso a la red. Tales problemas de seguridad no se limitan a un país concreto, sino que se extienden rápidamente a otros Estados miembros.

- Los Consejos Europeos de Feira y Lisboa reconocieron el papel de Internet como uno de los motores fundamentales de la productividad de las economías de la UE al lanzar el Plan de acción *e*Europa 2002.

En este contexto, el Consejo Europeo de Estocolmo de los días 23 y 24 de marzo de 2001concluyó que "*el Consejo, en concertación con la Comisión, pondrá en marcha una amplia estrategia en materia de seguridad de las redes electrónicas, que prevé medidas prácticas de aplicación. Esta estrategia deberá estar preparada para el Consejo Europeo de Gotemburgo."* La presente comunicación es la respuesta de la Comisión Europea a esta petición.

Un entorno cambiante

La seguridad se ha convertido en uno de los principales desafíos a que se enfrentan los responsables políticos y el estudio de una respuesta adecuada a este problema constituye una tarea cada vez más compleja. Hace tan solo unos años, la seguridad de la red era fundamentalmente un problema para los monopolios de Estado que ofrecían servicios especializados basados en redes públicas, fundamentalmente la red telefónica. La seguridad de los sistemas informáticos se limitaba a las grandes organizaciones y a los controles de acceso. La elaboración de una política de seguridad constituía una tarea relativamente fácil. La situación ha cambiado radicalmente debido a una serie de transformaciones producidas en el mercado mundial, entre las que cabe citar la liberalización, la convergencia y la mundialización.

En la actualidad predomina la propiedad y gestión privadas de las redes. Los servicios de comunicación están abiertos a la competencia y la seguridad forma parte de la oferta de mercado. No obstante, muchos clientes ignoran la amplitud de los riesgos en materia de seguridad a la hora de conectarse a la red y toman su decisión sin estar perfectamente informados.

Las redes y los sistemas de información están en un proceso de convergencia. Cada vez están más interconectados, ofrecen el mismo tipo de servicio sin descontinuidad y personalizado y comparten en cierta medida la misma infraestructura. Los equipos terminales (PC, teléfonos móviles, etc.) se han convertido en un elemento activo de la arquitectura de la red y pueden conectarse a distintas redes.

Las redes son internacionales. Una parte significativa de la comunicación actual es transfronteriza y transita por terceros países (a veces sin que el usuario final sea consciente de ello), por lo que cualquier solución a los problemas de seguridad habrá de tener en cuenta este factor. La mayoría de las redes están formadas por productos comerciales procedentes de proveedores internacionales. Los productos de seguridad deberán ser compatibles con las normas internacionales.

Pertinencia de la política

Todos estos factores limitan la capacidad de las administraciones públicas para influir en el nivel de seguridad de las comunicaciones electrónicas de ciudadanos y empresas. No obstante, ello no quiere decir que el sector público deje de tener una función que desempeñar. Estas son las razones que respaldan su papel:

En primer lugar, **existen varias medidas legales vigentes a escala comunitaria con repercusiones específicas en materia de seguridad de las redes y de la información.** En particular, el marco europeo de las telecomunicaciones y de la protección de los datos contiene disposiciones que obligan a los operadores y a los proveedores de servicios a garantizar un nivel de seguridad adecuado a los riesgos contemplados.

En segundo lugar, la **seguridad nacional** suscita cada vez más preocupación en la medida en que los sistemas de información y las redes de telecomunicaciones se han convertido en un factor crítico para otras infraestructuras (el abastecimiento de agua y electricidad, por ejemplo) y otros mercados (por ejemplo, el mercado financiero mundial).

Por último, existen varias razones que justifican la intervención pública para paliar las **deficiencias del mercado.** Los precios de mercado no siempre reflejan de forma exacta los costes y los beneficios de las inversiones en la mejora de la seguridad de las redes, y usuarios y proveedores no siempre soportan todas las consecuencias de sus prácticas. El control de la red es disperso y es posible utilizar los puntos débiles de un sistema para atacar a otro. La complejidad de las redes hace que los usuarios tengan dificultades para evaluar los peligros potenciales.

La presente Comunicación tiene pues por objetivo determinar en qué ámbitos es necesario introducir o reforzar la actuación pública a nivel europeo o nacional.

El capítulo 2 define la seguridad de las redes y de la información, describe las principales amenazas para la seguridad y evalúa las soluciones actualmente disponibles. Su intención es suministrar el nivel de comprensión de la seguridad de las redes y de la información suficiente para facilitar una buena comprensión de las soluciones propuestas. No se trata de ofrecer una visión técnica exhaustiva de los problemas de seguridad de las redes.

El capítulo 3 propone un enfoque político europeo dirigido a mejorar la seguridad de las redes y de la información. Se basa en un análisis de la necesidad de completar las soluciones del mercado con acciones a nivel político. Presenta una serie de medidas concretas, tal y como solicitó el

Consejo Europeo de Estocolmo. La política propuesta debe verse como parte integrante del marco existente para los servicios de comunicación electrónica, la protección de los datos y, más recientemente, la política en materia de *ciberdelincuencia*.

2. Análisis de los problemas de seguridad de las redes y de la información

2.1. Definición de la seguridad de las redes y de la información

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos. Están compuestos de elementos de tansmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y de servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.). Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc) y de equipos terminales (teléfono, ordenadores centrales, ordenadores personales, teléfonos móviles, organizadores personales, aparatos electrodomésticos, máquinas industriales, etc.).

Los requisitos generales de seguridad de las redes y los sistemas de información presentan las siguientes características generales interdependientes:

i) **Disponibilidad** – Significa que los datos son accesibles y los servicios operativos aún en caso de alteraciones del tipo de cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red de comunicaciones pueda provocar interrupciones en otras redes críticas como el transporte aéreo o el suministro de electricidad.

ii) **Autenticación** – Confirmación de la identidad declarada de usuarios o entidades jurídicas. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos (por ejemplo, para el teletrabajo) y la autenticación de los sitios Web (por ejemplo, en el caso de los bancos en Internet). La autenticación debe contemplar la posibilidad de mantener el **anonimato,** dado que muchos servicios no necesitan la identidad del usuario y sólo requieren la confirmación fiable de determinados criterios (las denominadas credenciales anónimas) como la capacidad de pago.

iii) **Integridad** – Confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica (datos médicos, diseño industrial, etc.).

iv) **Confidencilidad** – Protección de las comunicaciones o de los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es especialmente necesaria para la transmisión de datos sensibles y uno de los requisitos a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la seguridad, y no únicamente los de carácter malintencionado. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques malintencionados.

La seguridad de las redes y de la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de

confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

2.2. Resumen de las amenazas en materia de seguridad

Las empresas que utilizan la red para vender sus productos u organizar la entrega de los mismos pueden verse paralizadas por un ataque del tipo "denegación de servicio". La información personal y financiera puede ser interceptada y utilizada con fines fraudulentos. La seguridad nacional puede verse amenazada. Estos ejemplos dan una idea del peligro que supone una seguridad deficiente. Cabe distinguir entre ataques intencionados (secciones 2.2.1 a 2.2.5) y alteraciones no intencionadas (sección 2.2.6). El objetivo de estas secciones es especificar el tipo de riesgos para la seguridad con el fin de preparar un marco político para mejorar la seguridad en la sección 3.

2.2.1. Interceptación de las comunicaciones

La comunicación electrónica puede verse interceptada y los datos pueden ser copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, "pinchando" la línea, y el control de las transmisiones de radio. Los puntos críticos para la interceptación del tráfico de comunicación son los puntos de gestión y de concentración de la red, como los encaminadores, pasarelas, conmutadores y servidores de explotación de la red.

Es preciso distinguir la interceptación ilegal o malintencionada de las comunicaciones de las actividades legales de interceptación. La interceptación de las comunicaciones por razones de seguridad pública está autorizada en casos específicos y con fines limitados en todos los Estados miembros de la UE. Existe un marco jurídico que permite a los órganos encargados de hacer respetar la ley obtener una orden judicial o, en el caso de dos Estados miembros, una autorización expedida por un ministro, para interceptar las comunicaciones.

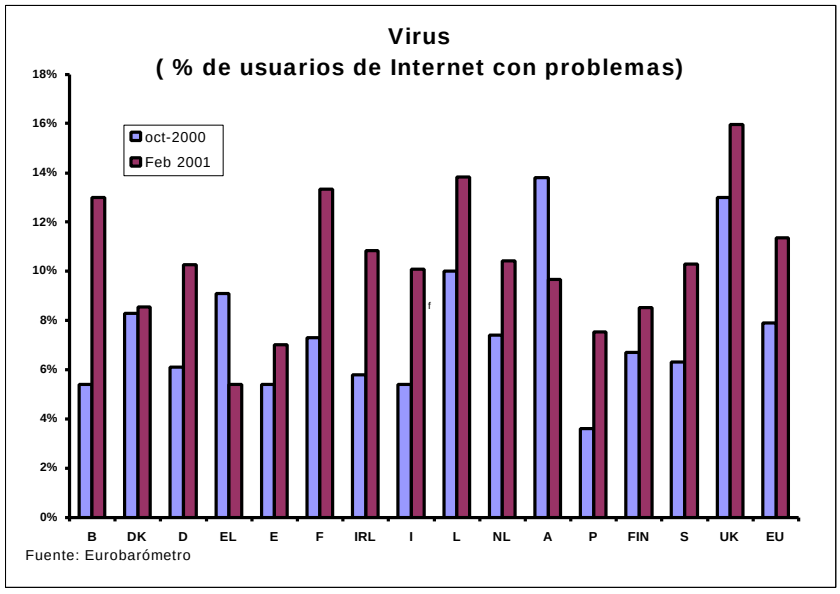
Daños potenciales - La interceptación ilegal puede causar daños tanto por intrusión en la vida privada de las personas como por la explotación de los datos interceptados, como palabras clave o datos de las tarjetas de crédito, para usos comerciales o sabotaje. Este es uno de los principales frenos del desarrollo del comercio electrónico en Europa.

Soluciones potenciales – La defensa contra la interceptación podrá realizarse a través de los **operadores** que deben velar por la seguridad de la red con arreglo a lo dispuesto en la Directiva 97/66 CE[1] y de los **usuarios** que pueden encriptar los datos transmitidos por la red.

Para los **operadores,** la protección de la red contra la interceptación es una tarea compleja y costosa. El método clásico utilizado por los operadores de servicios de telecomunicaciones para garantizar la seguridad de las redes han sido los controles del acceso físico de las redes en las instalaciones y directrices para el personal. La encripción del tráfico sólo se ha utilizado esporádicamente. Para las aplicaciones sin hilo, es preciso velar por que las transmisiones por radio estén adecuadamente encriptadas. Los operadores de servicios de comunicación móvil encriptan el tráfico entre el teléfono móvil y la estación de base. En la mayor parte de los países de la UE, la eficacia de la encripción está por debajo de las posibilidades técnicas debido a la necesidad de hacer posible la interceptación legal. Por las mismas razones, la encripción puede conectarse y desconectarse de las estaciones de base sin que lo sepa el usuario.

[1] Directiva sobre la protección de los datos en las telecomunicaciones (DO L 24 de 30.1.1998).

Los usuarios pueden decidir encriptar ellos mismos los datos o las señales de voz con independencia de las disposiciones de seguridad de la red. Aún en el caso de ser interceptados, los datos encriptados correctamente son incomprensibles para todo el mundo, excepto los destinatarios autorizados. Para casi todos los tipos de comunicación existen abundantes programas informáticos y material de encripción disponibles[2]. Existen productos especiales para encriptar una conversación telefónica o una transmisión por fax. El correo electrónico puede encriptarse gracias a un programa informático especial o por medio de un programa integrado en el programa de tratamiento de textos o un cliente del servicio de correo electrónico. Para el usuario, el problema reside en el hecho de que si encripta el correo electrónico o las comunicaciones vocales, el destinatario deberá poder entenderlo. Los equipos o los soportes lógicos deberán ser interoperables. También es preciso que conozcan la clave de de encripción, lo que significa que deberá existir un mecanismo para recibir la clave con la correspondiente autenticación de la misma. El coste de encripción en trabajo y dinero es importante y los usuarios a menudo no disponen de suficiente información sobre los riesgos y ventajas para la seguridad, lo que les impide tomar las decisiones adecuadas.



Un sistema de seguridad habitualmente utilizado en Internet es el denominado "Secure Socket Layer" (SSL), que encripta la comunicación entre un servidor web y el navegador del usuario. En el pasado, el desarrollo de esta tecnología, en particular su versión más potente (128 bit), se ha visto frenado por anteriores restricciones a su exportación por parte de los Estados Unidos. Recientemente se revisó el régimen de control de las exportaciones de los Estados Unidos a raíz de la adopción de un régimen comunitario más liberal para el control de las exportaciones de productos y tecnología de doble uso[3]. Las estadísticas señalan que el número de servidores web seguros en Europa está por debajo del de los Estados Unidos (ver gráfico).

Operadores, usuarios y productores deben hacer frente al problema de la diversidad de normas competidoras y no interoperables. Por ejemplo, en el ámbito de la seguridad del correo electrónico dos normas [4] compiten por hacerse con la hegemonía del mercado. La influencia de Europa en este campo ha sido escasa. Como consecuencia, el usuario europeo se enfrenta a una profusión de productos no europeos que emplean estas normas cuyo acceso puede verse restringido en función de la política de control de la exportación de los EE. UU. Dado que el

[2] Ver la Comunicación de la Comisión sobre "Fomento de la seguridad y la confianza en la comunicación electrónica" de 8 de octubre de 1997, COM (1997) 503 final

[3] Reglamento (CE) Nº 1334/2000 por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnología de doble uso.

[4] S-MIME (secure multiple Internet mail extensions) y OpenPGP (Pretty Good Privacy) son dos normas IETF (Internet Engineering Task Force).

nivel de seguridad que ofrece un buen número de estos productos (por ejemplo, Echelon[5]) suscita preocupación, algunos gobiernos de la UE están considerando la utilización de soportes lógicos de fuente abierta para reforzar la confianza en los productos de encripción. No obstante, estas iniciativas se encuentran aún en fase piloto[6], aún no han sido coordinadas y cabe incluso la posibilidad de que las fuerzas del mercado sean más fuertes que los esfuerzos gubernamentales aislados. La mejor forma de abordar este problema es una evaluación en profundidad de los productos comerciales y de fuente abierta.

2.2.2. Acceso no autorizado a ordenadores y redes de ordenadores.

El acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma malintencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques de diccionario, ataques de fuerza brutal (aprovechando la tendencia de la gente a utilizar contraseñas previsibles), ingeniería social (aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiables) e interceptación de contraseñas. Esta intrusión a menudo se produce desde dentro de la organización (ataques internos).

Daños potenciales - Si bien algunas intrusiones no autorizadas están motivadas por un desafío intelectual más que por un fin lucrativo, lo que empezó siendo una actividad molesta (a menudo llamada "hacking") ha puesto de manifiesto la vulnerabilidad de las redes de información y ha incitado a las personas con intenciones delictivas o malintencionadas a explotar los mismos puntos débiles. Todos los usuarios tienen derecho a la protección frente al acceso no autorizado a su información confidencial, en particular sus datos financieros, sus cuentas bancarias y sus historiales médicos. Para el sector público y empresarial, las amenazas van desde el espionaje económico a la modificación de los datos internos o públicos, incluida la corrupción de sitios Web.

Soluciones potenciales – Los métodos más ampliamente utilizados para protegerse contra el acceso no autorizado son los controles de contraseña y la instalación de cortafuegos. Estas soluciones ofrecen una protección limitada y deben completarse con otros controles de seguridad, por ejemplo el reconocimiento de ataques, la detección de intrusiones y el control a nivel de las aplicaciones (incluidos los sistemas que emplean tarjetas inteligentes). La eficacia de los controles depende de la correspondencia entre su funcionalidad y los riesgos relacionados con un entorno específico. Es preciso establecer un equilibrio entre la protección de la red y las ventajas del libre acceso. Debido a la rápida evolución de la tecnología y de los correspondientes nuevas amenazas para las redes, los controles independientes de la seguridad de las redes deberán ser revisados permanentemente. Mientras los usuarios y los proveedores no sean plenamente conscientes de la vulnerabilidad de sus redes, no se recurrirá plenamente a las posibles soluciones. El gráfico de más abajo ofrece una visión general de la utilización actual de los productos de seguridad en la Unión Europea (las estadísticas se basan en una encuesta realizada en febrero de 2001 en el marco del ejercicio de evaluación comparativa de la iniciativa *e*Europa 2002).

2.2.3. Perturbación de las redes

Actualmente las redes se encuentran ampliamente digitalizadas y controladas por ordenadores. En el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema

---

[5] El sistema ECHELON se usa en principio para interpretar comunicaciones de correo electrónico, fax y teléfono transmitidas por las redes de telecomunicaciones mundiales. Ver también las actividades del Comité temporal del Parlamento Europeo sobre Echelon en http://www.europarl.eu.int/committees/echelon_home.htm

[6] El gobierno alemás está financiando un proyecto basado en la norma OpenPGP denominado GNUPG (http://www.gnupg.org).

informático que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos suelen cebarse en los puntos débiles y más vulnerables de los componentes de las redes (sistemas operativos, encaminadores, conmutadores, servidores de nombres de dominio, etc.)

Si bien los ataques al sistema telefónico no han constituido una gran preocupación en el pasado, los ataques a Internet se han hecho bastante frecuentes. Esto se debe al hecho de que las señales de control telefónicas están separadas del tráfico y pueden ser protegidas, mientras que Internet permite a los usuarios acceder a los ordenadores clave de gestión. No obstante, la red telefónica puede hacerse más vulnerables en el futuro en la medida en que pueda integrar elementos clave de Internet y su plan de control esté abierto a agentes externos.

Los ataques pueden ser de varios tipos:

- **Ataques contra los servidores de nombres de dominio**: Internet depende del funcionamiento del sistema de nombres de dominio (DNS) por medio del cual se traducen direcciones de la red abstractas (por ejemplo, IP n° 147.67.36.16) en nombres comprensibles (por ejemplo, www.europa.eu.int) y viceversa. Si falla una parte del DNS no se podrán localizar algunos sitios Web y los sistemas de envío del correo electrónico podrán dejar de funcionar. La corrupción de los servidores raíz DNS u otros servidores de nombres de dominio de nivel superior podría provocar una perturbación general. A principios del presente año, se han descubierto ciertos puntos débiles en los programas utilizados por la mayor parte de los servidores de nombres de dominio.[7]

- **Ataques contra el sistema de encaminamiento**: El encaminamiento en Internet está altamente descentralizado. Cada encaminador informa periódicamente a los encaminadores cercanos de las redes que conoce y de la forma de alcanzarlas. El peligro está en que estas informaciones no pueden ser verificadas ya que, debido al diseño del sistema, el conocimiento que cada encaminador tiene de la topología de la red es mínimo. Por consiguiente, cualquier encaminador puede presentarse a sí mismo como el mejor camino a un destino determinado con el fin de interceptar, bloquear o modificar el tráfico a ese destino.

- **Ataques por saturación y denegación de servicio**: Estas formas de ataque atentan contra la red sobrecargándola con mensajes artificiales que dificultan o impiden el acceso legítimo. Se podría comparar con el caso de un fax bloqueado por mensajes largos y repetidos. Los ataques por saturación tratan de sobrecargar los servidores Web o la capacidad de tratamiento de los proveedores de servicios de Internet por medio de mensajes generados automáticamente.

Daños potenciales - Las interrupciones han perjudicado a algunos sitios Web prestigiosos. Algunos estudios han estimado en varios cientos de millones de euros el coste de un ataque reciente, sin contar el perjuicio no cuantificable en términos de reputación. Las empresas cuentan cada vez más con la disponibilidad, de su sitio Web para sus negocios, siendo especialmente vulnerables las que dependen de el para el suministro *just in time*.

Soluciones potenciales - Los ataques contra los servidores DNS son en principio fáciles de combatir si se extienden los protocolos DNS, por ejemplo con ayuda de extensiones DNS seguras basadas en la criptografía de clave pública. No obstante, ello exige la instalación de nuevos programas informáticos en las máquinas clientes, por lo que aún no está suficientemente

[7] Fuente CERT/CC at http://www.cert.org/advisories/CA-2001-02.html

extendido. Además, el proceso administrativo necesario para aumentar la confianza entre los dominios DNS debe hacerse más eficaz.

Los ataques contra el sistema de encaminamiento son mucho más difíciles de combatir. Internet ha sido diseñado para favorecer al máximo la flexibilidad de encaminamiento con el fin de reducir la probabilidad de pérdida de un servicio en caso de fallo de una parte de la infraestructura de la red. No existe ningún medio eficaz para dar seguridad a los protocolos de encaminamiento, en particular en los encaminadores principales.

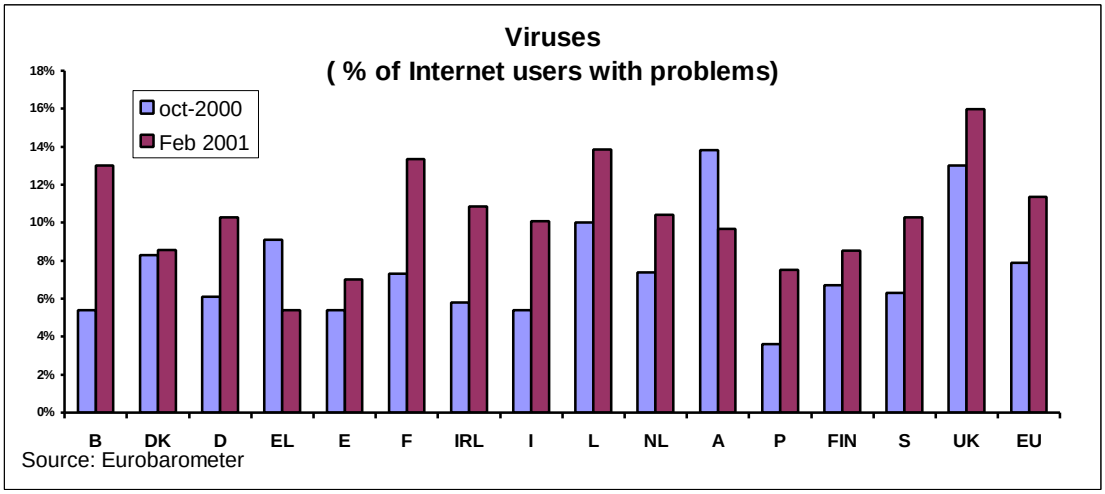
El volumen de los datos transmitidos no permite un filtrado pormenorizado, dado que tal verificación llevaría al colapso de la red. Por esta razón las redes sólo incluyen funciones elementales de filtrado y de control de acceso, mientras que las funciones de seguridad más elaboradas (autenticación, integridad, encripción, por ejemplo) se sitúan en la frontera de las redes, es decir, en las terminales y servidores de las redes que sirven de puntos terminales.

2.2.4. Ejecución de programas malintencionados que modifican y destruyen los datos

Los ordenadores funcionan con programas informáticos. Lamentablemente, los programas pueden usarse también para desactivar un ordenador y para borrar o modificar los datos. Como ya se ha explicado, cuando esto ocurre en un ordenador que forma parte de la gestión de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Un virus es un programa informático malintencionado. Es un programa que reproduce su propio código adhiriéndose a otros programas de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.

Existen otros tipos de software maligno: algunos afectan únicamente al ordenador en el que se copian, mientras que otros se propagan a otros ordenadores conectados en la red. Por ejemplo, existen programas (denominados "bombas lógicas") que permanecen en letargo hasta que son activados por un acontecimiento específico, como una fecha (por ejemplo, viernes 13). Otros programas parecen benignos pero cuando se lanzan ponen en marcha un ataque maligno ("caballos de Troya"). Otros programas (denominados "gusanos") no infectan otros programas como si se tratara de un virus, sino que crean copias de ellos mismos, copias que crean a su vez más copias que acaban inundando el sistema.

Daños potenciales - Los virus pueden ser muy destructivos como ponen de relieve los elevados costes que originaron recientes ataques (por ejemplo, "I Love You", "Melissa" y "Kournikova"). El gráfico que se muestra más adelante ofrece un resumen del aumento del número de virus que los usuarios de Internet de la UE encontraron entre octubre de 2000 y febrero de 2001 (por Estado miembro). Una media del 11% de los usuarios de Internet europeos atraparon un virus en su ordenador doméstico.



Soluciones potenciales - Los programas antivirus son la única defensa. Están disponibles en varias modalidades. Por ejemplo, los escáner y desinfectantes de virus identifican y borran los virus conocidos. Su principal debilidad reside en el hecho de que no identifican fácilmente nuevos virus aun cuando se actualicen regularmente. Otro ejemplo de defensa antivirus lo constituye el comprobador de la integridad. Para que un virus pueda infectar un ordenador debe cambiar alguna cosa en ese sistema. El control de integridad permitiría identificar dichos cambios del sistema aun cuando los produzca un virus desconocido.

A pesar de la existencia de productos de defensa relativamente bien desarrollados, han aumentado los problemas creados por los programas malignos. Dos son las razones principales: en primer lugar, el grado de apertura de Internet permite que los piratas aprendan los unos de los otros y desarrollen métodos para eludir los mecanismos de protección; en segundo lugar, Internet se extiende y llega a un número cada vez mayor de usuarios, muchos de los cuales no se dan cuenta de la necesidad de tomar precauciones. La seguridad dependerá del grado de difusión de los programas de protección.

2.2.5. Declaración falsa

A la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. La red ofrece algunas indicaciones, pero el mayor riesgo de ataque procede de la gente que conoce el contexto, es decir, los "***insiders".*** Cuando un usuario marca un número o teclea una dirección Internet en el ordenador, debería alcanzar el destino previsto. Esto es suficiente para un gran número de aplicaciones, pero no para las transacciones comerciales importantes o las comunicaciones médicas, financieras u oficiales, que exigen un nivel más elevado de integridad, autenticación y confidencialidad.

Daños potenciales - Las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos. Los usuarios pueden descargar programas malignos de un sitio Web que se presenta como una fuente fiable. Programas de rechazo de este tipo pueden transmitir datos confidenciales a personas no autorizadas. La declaración falsa puede ser la causa del rechazo de un contrato, etc. El daño principal es sin duda el hecho de que la falta de autenticación constituya un freno a posibles transacciones comerciales. Numerosos estudios señalan que las preocupaciones en materia de seguridad constituyen una de las principales razones para no llevar a cabo transacciones por Internet. Si la gente pudiera confiar plenamente en que su interlocutor es quien afirma ser, el nivel de confianza en las transacciones de Internet aumentaría sensiblemente.

Soluciones potenciales - Los esfuerzos por introducir la autenticación en las redes, junto con el protocolo SSL, ya permiten garantizar un cierto grado de confidencialidad. Las redes privadas virtuales (VPN) utilizan SSL e IPsec para permitir comunicaciones en Internet y en canales abiertos con un grado determinado de seguridad. No obstante, la utilidad de estas soluciones se ve limitada en la medida en que se basan en certificados electrónicos y que no existe ninguna garantía sobre la autenticidad de los mismos. Un tercero, a menudo denominada "autoridad de certificación" o, como en el caso de la Directiva sobre firmas electrónicas[8], "proveedor de servicios de certificación", puede ofrecer dicha garantía. La adopción a gran escala de esta solución se enfrenta al mismo problema que la encripción, la necesidad de interoperabilidad y de llevar a cabo una gestión de las claves. En una VPN esto no es un problema, ya que se pueden desarrollar soluciones pa4tentadas, sin embargo, en el caso de las redes públicas se trata de un problema de gran importancia.

La Directiva sobre firmas electrónicas mejora el fundamento jurídico para facilitar la autenticación electrónica en la UE. Constituye un marco que permite el desarrollo libre del mercado, pero que incluye disposiciones que fomentan el desarrollo de firmas más seguras para su reconocimiento legal. La transposición de la Directiva al Derecho nacional está actualmente en curso.

2.2.6. Accidentes no provocados

Numerosos problemas de seguridad se deben a accidentes imprevistos o no provocados como:

- catástrofes naturales (por ejemplo, tormentas, inundaciones, incendios, terremotos)
- terceras partes sin relación contractual con el operador o el usuario (por ejemplo, interrupción del servicio por obras de construcción)
- terceras partes con relación contractual con el operador o el usuario (defectos de programas informáticos o componentes de ordenadores suministrados)
- errores humanos o deficiencias de la gestión del operador (incluido el proveedor de servicio) o el usuario (por ejemplo, problemas en la gestión de la red o incorrecta instalación de un programa).

Daños potenciales: Las catástrofes naturales pueden perturbar la disponibilidad de las redes. Es en dichos casos cuando, por desgracia, se hace fundamental justamente disponer de líneas de comunicación en perfecto estado. Las averías del soporte físico y las deficiencias del diseño del soporte lógico pueden provocar la alteración inmediata del servicio o favorecer los ataques. Una gestión deficiente de la capacidad de la red puede provocar una congestión que ralentice o obstruya los canales de comunicación.

En este contexto, una cuestión crucial la constituye la distribución de responsabilidades entre las partes. En la mayoría de los casos los usuarios están exentos de responsabilidades, pero las posibilidades de presentar una reclamación son escasas o nulas.

Soluciones potenciales: Los operadores de las redes de telecomunicaciones conocen los riesgos de accidentes del entorno y para ello han previsto redundancias y protección de la infraestructura en sus redes. El aumento de la competencia podrían tener un impacto ambivalente en la conducta de los operadores. Por un lado, la competitividad de los precios puede empujar a los operadores a

[8] Directiva 1999/93/CE de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica (DO L 13 de 19.1.2000, p. 12).

reducir estas redundancias, pero por otro, el aumento en el número de operadores como resultado de la liberalización del mercado puede hacer que los usuarios pasen a un nuevo operador en caso de no disponibilidad del suyo (del mismo modo que se cambia de compañía a un pasajero cuando se anula el vuelo de la compañía en la que viajaba). No obstante, el Derecho comunitario obliga a los Estados miembros a tomar los pasos necesarios para garantizar la disponibilidad de las redes públicas en caso de catástrofes naturales u otra interrupción accidental de la red (Directiva 97/33/CE sobre interconexión[9] y Directiva 98/10/CE sobre telefonía vocal[10]). En conjunto, en este ámbito, poco se sabe sobre el nivel de seguridad como resultado del aumento del número de redes interconectadas.

La competencia entre los proveedores de soportes y programas informáticos debería repercutir en la mejora de la seguridad de los productos, sin embargo, la competencia no es lo suficientemente fuerte como para favorecer las inversiones en materia de seguridad y ésta última tampoco constituye un factor de compra clave. Los defectos de seguridad se advierten a menudo demasiado tarde, cuando el daño ya es irreparable. La defensa de la competencia leal en los mercados de la tecnología de la información favorecerá el desarrollo de condiciones de seguridad adecuadas.

El riesgo de errores humanos y de funcionamiento puede reducirse mejorando la información y la concienciación. El establecimiento de una política adecuada en materia de seguridad a nivel de la empresa podría reducir estos riesgos.

2.3. Nuevos desafíos

La seguridad de la red y de la información se convertirá probablemente en un factor clave del desarrollo de la sociedad de la información dado medida que el desarrollo de las redes desempeña un papel fundamental en la vida económica y social. Dos son los temas principales que habrá que considerar: el aumento del daño potencial y la aparición de nuevas tecnologías:

i) Las redes y sistemas de información transportan cada vez más **datos sensibles e información económica valiosa** que los hace objeto potencial de ataques. Estos ataques son de poca importancia y de escasa gravedad a escala nacional, por ejemplo en el caso de la degradación de un sitio Web personal o del reformateado de un disco duro por parte de un virus. No obstante, la perturbación se puede producir a otra escala mucho más crítica, hasta plantear problemas como interferencias en las comunicaciones militares, graves cortes de corriente o importantes pérdidas comerciales debidas a ataques por denegación de servicio o de violaciones de la confidencialidad.

   Es difícil evaluar el alcance exacto de los daños reales y potenciales imputables a deficiencias de la seguridad de las redes. No se dispone de un sistema de información sistemático y muchas empresas prefieren ocultar los ataques sufridos para evitar una publicidad negativa. Por todo ello, las pruebas de que se disponen son puramente anecdóticas. Los costes de los ataques no son sólo los costes directos (pérdida de ingresos, pérdida de información valiosa, costes de mano de obra para la reparación de la red), sino también los intangibles, más difíciles de estimar, de los que el principal es la pérdida de reputación.

ii) **La seguridad de las redes es un problema dinámico**. La velocidad en el cambio de la tecnología plantea nuevos desafíos de forma permanente. Los problemas que ayer se planteaban desaparecen y las soluciones actuales de dichos problemas dejan de tener sentido. Casi cada día aparecen en el mercado aplicaciones, servicios y productos nuevos. Pero es

[9] DO L 199 de 26.07.1997.
[10] DO L 101 de 01.04.1998.

evidente que algunos factores del desarrollo de las redes suponen un importante desafío para una política de la seguridad privada y pública:

- Diferentes objetos digitales transitarán por las redes, como objetos multimedios, programas descargables o agentes móviles con políticas de seguridad incorporadas. La noción de disponibilidad tal y como hoy se percibe como la posibilidad de usar las redes evolucionará en términos de uso autorizado, por ejemplo, el derecho de utilizar un juego de vídeo durante un tiempo determinado, el derecho a crear una única copia de un programa informático, etc.

- En el futuro, los operadores de las redes de IP podrán querer aumentar la seguridad recurriendo al control continuo del tráfico de la red, con el fin de permitir únicamente el tráfico autorizado. No obstante, estas medidas deberán ajustarse a las correspondientes normas de protección de los datos.

- Los usuarios pasarán a disponer de conexiones de Internet activas y permanentes lo que multiplicará los riesgos de piratería y hará vulnerables los terminales no protegidos, al tiempo que será más fácil para los piratas evitar la detección.

- Se generalizará el uso de redes domésticas que conecten varios aparatos, lo que ofrecerá nuevas posibilidades de ataque y aumentará la vulnerabilidad de los usuarios (desactivación de alarmas a distancia, por ejemplo).

- La introducción a gran escala de redes sin hilos (por ejemplo, bucle local inalámbrico, redes de área local inalámbrica y móviles de la tercera generación) planteará el problema de la encripción de las señales de radio. Por lo tanto, resultará cada vez más difícil exigir por ley una encripción leve de dichas señales.

- Las redes y los sistemas de información estarán en todas partes, con una combinación de sistemas fijos y sin hilo, y ofrecerán un "ambiente inteligente", es decir, funciones autoorganizadas activadas de forma automática que tomarán decisiones que antes tomaba el usuario. El reto será evitar debilidades inaceptables e integrar la arquitectura de seguridad.

3. Un enfoque político europeo

3.1. Justificación de la intervención pública

La protección de las redes de comunicación constituye cada vez más una prioridad para los responsables políticos debido a la necesidad de proteger datos, de garantizar el funcionamiento de la economía, por motivos de seguridad nacional y el deseo de promocionar el comercio electrónico. Ello ha favorecido la aparición de un importante cuerpo de salvaguardas legales en las Directivas de la UE sobre protección de los datos y en el marco reglamentario de la UE en materia de telecomunicaciones (como se demuestra en la sección 3.6). Estas medidas se deberán aplicar no obstante en un entorno cambiante de nuevas tecnologías, mercados competitivos, convergencia de redes y globalización. Estos desafíos se ven agravados por el hecho de que el mercado tiende a no invertir lo suficiente en seguridad por razones ya indicadas.

Las seguridad de las redes y de la información constituye una mercancía que se vende y compra en el mercado y que forma parte de las cláusulas contractuales. El mercado de los productos de seguridad ha registrado una crecimiento sustancial a lo largo de los últimos años. Según algunos estudios, el mercado mundial de programas informáticos de seguridad para Internet se estimaba

en 4,4 millardos de dólares a finales de 1999[11] y crecerá un 23% anual hasta alcanzar 8,3 millardos de dólares en 2004. En Europa, se estima que el mercado de la seguridad de las comunicaciones electrónicas pasará de 465 millones de dólares en 2000 a 5,3 millardos de dólares en 2006[12], mientras que el mercado de la seguridad para las tecnologías de la información pasará de 490 millones de dólares en 1999 a 2,74 millardos de dólares en 2006 [13].

Se suele pensar que el juego del mercado equilibrará los costes del suministro de servicios de seguridad y la necesidad específica de seguridad. Algunos usuarios solicitarán mucha seguridad mientras que otros estarán satisfechos con un nivel menos alto de garantía, si bien el Estado podría garantizar un nivel mínimo de seguridad. Sus preferencias se reflejarán en el precio que estén dispuestos a pagar por los elementos de seguridad. No obstante, como se puso de relieve en la sección 2, muchos riesgos de seguridad siguen sin estar resueltos o las soluciones a ciertos problemas de seguridad tardan en comercializarse precisamente debido a las deficiencias del funcionamiento del mercado.

i) **Costes y beneficios sociales:** La inversión en la mejora de la seguridad de la red genera unos costes sociales que no están adecuadamente reflejados en los precios del mercado. **Por lo que se refiere a los costes,** los agentes del mercado no son responsables de todas las responsabilidades que se desprenden de su comportamiento en materia de seguridad. Los usuarios y proveedores con un nivel de seguridad escaso no corren a cargo de la responsabilidad civil. Sería el caso de un automovilista temerario al que no se hace responsable de los costes del embotellamiento que provoca su accidente. Del mismo modo, en Internet varios ataques se han producido a través de máquinas desprotegidas de usuarios relativamente descuidados. **Los beneficios de la seguridad tampoco están plenamente reflejados en los precios del mercado.** Cuando los operadores, fabricantes o proveedores de servicios mejoran la seguridad de sus productos, una gran parte de los beneficios de esta inversión repercuten no sólo en sus clientes, sino también en todos los directa o indirectamente afectados por las comunicaciones electrónicas, básicamente toda la economía.

ii) **Asimetría de información:** Las redes son cada vez más complejas y alcanzan un mercado cada vez más amplio que incluye a un gran número de usuarios con escasos conocimientos por lo que se refiere a la tecnología y los riesgos potenciales. Esto significa que los usuarios no son plenamente conscientes de los riesgos en materia de seguridad y que muchos operadores, fabricantes y proveedores de servicios tienen dificultades para evaluar la existencia y difusión de vulnerabilidades. Muchos servicios, aplicaciones y programas nuevos ofrecen prestaciones atractivas que a menudo son fuente de nuevas vulnerabilidades (por ejemplo, el éxito de las Web mundiales se debe en parte a la gama de aplicaciones multimedia que pueden teledescargarse fácilmente, pero estos "plug ins" son también un punto de entrada de ataques). Si bien los beneficios son visibles, los riesgos no lo son y los existen más incentivos para que los proveedores ofrezcan nuevas prestaciones en lugar de más seguridad.

iii) **El problema de la intervención pública:** Los operadores adoptan cada vez más las normas de Internet o conectan de algún modo sus redes a Internet. No obstante, la seguridad no inspiró el diseño de Internet, más bien al contrario, se desarrolló para garantizar el acceso a la información y para facilitar su intercambio. Este ha sido el motivo de su éxito. Internet se ha convertido en una red de redes mundial de una riqueza y diversidad sin precedentes, amorfa y carente de parámetros precisos. Las inversiones en seguridad a

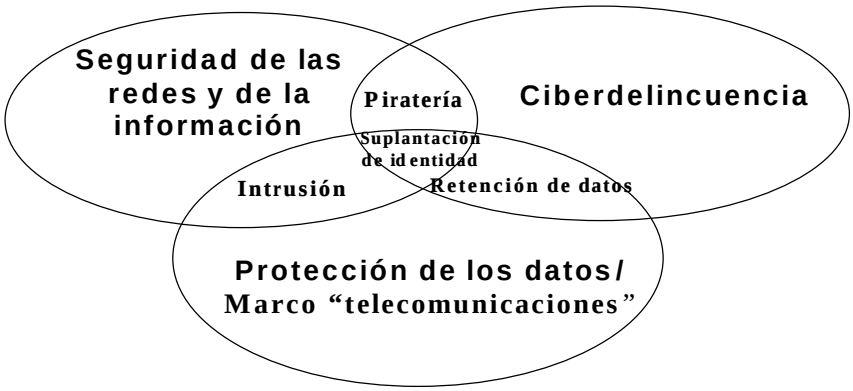
[11] IDC : Internet security market forecast and analysis, 2000-2004 Report #W23056 - October 2000
[12] Frost&Sullivan : The European Internet communication security markets, report 3717 - November 2000
[13] Frost&Sullivan : The European Internet system security markets, report 3847 - July 2000

menudo son sólo útiles si hace lo mismo un número suficiente de gente. Por lo tanto, es necesario **cooperar** para establecer soluciones de seguridad. La cooperación sólo funciona con una masa crítica de jugadores, lo que no es fácil de conseguir dado que los beneficios son para todos, aún para quienes no inviertan en seguridad. La interoperabilidad entre productos y servicios abrirá las puertas a la competencia entre las distintas soluciones en materia de seguridad. No obstante, los costes de coordinación son importantes en el caso de soluciones globales y algunos agentes se ven tentados a imponer una solución patentada en el mercado. Dado que muchos productos y servicios aún utilizan soluciones patentadas, no hay ninguna ventaja competitiva en usar normas de seguridad que sólo son eficaces si su uso es universal.

Como resultado de estas imperfecciones el marco de protección de los datos y de las telecomunicaciones ya estipula una serie de obligaciones para los operadores y proveedores de servicios para garantizar un determinado nivel de seguridad en los sistemas de información y comunicación. La justificación de una intervención a escala europea en materia de seguridad de las redes y de la información puede describirse de la forma siguiente. En primer lugar, las disposiciones legales de la UE han de aplicarse de forma eficaz, lo que exige **una comprensión común de los problemas de seguridad latentes y de las medidas específicas a adoptar.** El marco legal deberá evolucionar también en el futuro, como ya puede verse en el caso del nuevo marco reglamentario propuesto para las comunicaciones electrónicas o en el de las próximas propuestas en materia de cibercriminalidad. En segundo lugar, algunas imperfecciones del mercado conducen a la conclusión de que las fuerzas del mercado no encauzan las inversiones necesarias hacia el desarrollo de tecnologías de las seguridad o a prácticas de seguridad. **Las medidas políticas pueden reforzar el proceso del mercado y mejorar al mismo tiempo el funcionamiento del marco legal.** Por último, los servicios de comunicación y de información son transfronterizos, lo que exige un enfoque europeo para **garantizar un mercado único para estos servicios, el aprovechamiento de las soluciones comunes y la capacidad para actuar de forma eficaz a nivel mundial.**

Las medidas políticas propuestas en materia de seguridad de las redes y de la información deberán considerarse no solamente en el contexto de la legislación existente en materia de telecomunicación y protección de los datos, sino también en relación con las políticas más recientes de lucha contra la ciberdelincuencia. La Comisión publicó recientemente una Comunicación sobre la ciberdelincuencia[14] en la que se prevé, entre otras iniciativas, el establecimiento de un foro UE de ciberdelincuencia de fomento de la comprensión y cooperación a nivel de la UE de todas las partes afectadas. Una política de seguridad de las redes y de la información será el eslabón perdido en este marco político. El siguiente diagrama muestra las tres áreas e ilustra con algunos ejemplos su interrelación.

[14] Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, COM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html



3.2. Concienciación

Demasiados usuarios (públicos y privados) aún no son conscientes de las posibles amenazas a que se pueden enfrentar a la hora de usar las redes de comunicación o las soluciones que ya existen para hacerles frente. Los temas de seguridad son complicados y la evaluación de los riesgos es difícil incluso para los expertos. La falta de información es una de las imperfecciones del mercado que una política de seguridad debería paliar. Existe el riesgo de que muchos usuarios, alarmados ante la información sobre los problemas de seguridad, renuncien al comercio electrónico sin más. Otros que no estén suficientemente informados o que subestimen el riesgo pueden ser poco cuidadosos. Algunas empresas podrían verse tentadas a quitar importancia a algunos riesgos ante el temor de perder clientes potenciales.

Paradójicamente existe una gran cantidad de información sobre seguridad de las redes y de la información disponible en Internet y las revistas informáticas cubren este tema sobradamente. El problema para los usuarios es encontrar información adecuada y comprensible, actualizada y que responda a sus necesidades prácticas. La industria del automóvil ofrece un buen ejemplo de como complicadas especificaciones en materia de seguridad se pueden transformar en una prestación clave para obtener una ventaja comercial. Por último, los proveedores de servicios de un servicio de telecomunicaciones público están obligados, con arreglo a la legislación comunitaria, de informar a sus subcriptores sobre los riesgos específicos de un fallo en la seguridad de la red y de los posibles remedios, incluidos los costes correspondientes (artículo 4 de la Directiva 97/66/CE).

El objetivo de una iniciativa de concienciación de los ciudadanos, administraciones y empresas es por lo tanto suministrar información accesible, independiente y fiable sobre seguridad de la red y de la información. Es preciso un debate sobre seguridad. Una vez garantizada la concienciación, la gente puede optar por el nivel de protección que crea conveniente.

Acciones propuestas:

- Los Estados miembros deberán poner en marcha una campaña de información y de educación y es preciso actualizar el trabajo en marcha en este sentido. Debería tratarse de una campaña en los medios de comunicación de masas dirigida a las partes interesadas. Una campaña buena y eficaz no es barata. El desarrollo de un contenido que no sea alarmista y que no ofrezca nuevas pistas a piratas potenciales exige una planificación cuidadosa.

La Comisión Europea facilitará un intercambio de las mejores prácticas y garantizará un determinado nivel de coordinación de las distintas campañas nacionales a nivel comunitario, en concreto en lo que se refiere al contenido de la información que deberá ofrecerse. Un elemento de esta acción será un portal para sitios Web tanto a nivel nacional como europeo. La conexión de estos portales con sitios Web fiables de socios internacionales también está prevista.

- Los Estados miembros deberán fomentar el uso de mejores prácticas basadas en medidas existentes como ISO/IEC 17799 (código de prácticas para la gestión de la seguridad de la información www.iso.ch). Esta medida debería estar especialmente dirigida a las PYME. La Comisión prestará su apoyo a los Estados miembros en estos esfuerzos.

- Los sistemas de educación de los Estados miembros deberán prestar mayor atención a los cursos sobre seguridad. Deberán desarrollarse programas educativos a todos los niveles, con formación sobre los riesgos de seguridad de redes abiertas y soluciones eficaces, como parte de la enseñanza de informática de las escuelas.

  Es preciso que los profesores aprendan sobre seguridad en sus programas de formación. La Comisión Europea apoya el desarrollo de nuevos módulos para los planes de estudios en el contexto de su programa de investigación.

3.3. Un sistema europeo de alarma y de información

Aún cuando los usuarios conozcan los riesgos para la seguridad seguirá siendo preciso alertarles sobre nuevos peligros. Los piratas siempre encontrarán nuevos flancos débiles en los sistemas de protección. La industria desarrolla permanentemente nuevas aplicaciones y servicios informáticos que ofrecen servicios de mejor calidad y hacen Internet más atractivo, pero este proceso también abre nuevas brechas de forma involuntaria.

Incluso los ingenieros de redes y los expertos informáticos se sorprenden con la novedad de algunos ataques. Es necesario establecer un sistema rápido de alarma que pueda alertar rápidamente a todos los usuarios, junto con una fuente de información rápida y fiable sobre cómo hacer frente a los ataques. Las empresas también necesitan un mecanismo fiable para poder informar de los ataques sin correr el riesgo de perder la confianza del público. A ello debe contribuir también un análisis de la seguridad más amplio y a más largo plazo que aúne el estudio de las pruebas y la evaluación de los riesgos con los beneficios de una perspectiva más amplia.

Gran parte del trabajo en este área lo realizan los equipos de respuesta para emergencias informáticas (CERT) o entidades similares. Por ejemplo, Bélgica ha puesto en pie un sistema de alerta antivirus que permite informar a los ciudadanos belgas de las amenazas de virus en un plazo de dos horas. Los CERT existentes operan de forma diferente en cada Estado miembro, lo que hace la cooperación bastante complicada. Los CERT existentes no están siempre convenientemente equipados y sus tareas a menudo no están claramente definidas. La coordinación mundial se realiza a través de CERT/CC, parcialmente financiada por el gobierno de los Estados Unidos y los CERT europeos dependen de la política de difusión de la información del CERT/CC y otros.

Como consecuencia de estas dificultades la cooperación europea es bastante limitada. La cooperación es fundamental para garantizar una alarma precoz en toda la Unión a través del intercambio instantáneo de información desde los primeros signos de ataque en un país. Por lo tanto, sería preciso fortalecer la cooperación con el sistema CERT en la Unión Europea con carácter urgente. En el contexto del plan de acción *e*Europa, se ha acordado una primera acción dirigida al fortalecimiento de la cooperación entre el sector público y privado en materia de

seguridad de funcionamiento de las infraestructuras de información (incluido el desarrollo de sistemas de alarma precoz) y la mejora de la cooperación entre los distintos CERT.

Acciones propuestas:

- Los Estados miembros deberán revisar su sistema de CERT con el fin de mejorar el equipamiento y competencias de los centros existentes. Como apoyo al trabajo nacional en este sentido, la Comisión Europea desarrollará una propuesta concreta para fortalecer la cooperación en la Unión Europea. Dicho apoyo incluirá las propuestas de proyectos en el marco del programa TEN Telecom que garanticen la creación eficaz de redes y el establecimiento de medidas de acompañamiento en el programa TSI con el fin de facilitar el intercambio de información.

- Una vez creada la red CERT a nivel de la UE, se debería conectar a instituciones similares a nivel mundial, por ejemplo al sistema de información de incidentes del G8 propuesto.

- La Comisión propone que se examine con los Estados miembros la forma óptima de organizar la recogida de datos a nivel europeo, su análisis y la planificación de futuras respuestas a las amenazas para la seguridad emergentes. El carácter organizativo de una posible estructura es una cuestión a debatir con los Estados miembros.

3.4. Apoyo tecnológico

La inversión en soluciones en materia de seguridad de las redes y de la información en la actualidad no es la óptima tanto por lo que se refiere al uso de tecnología como a la investigación de nuevas soluciones. En un contexto en el que la aparición de nuevas tecnologías trae consigo inevitablemente nuevos riesgos, es vital una investigación permanente.

La seguridad de la red y de la información ya figura en el programa relativo a las Tecnologías de la Sociedad de la Información (TSI) del 5º Programa Marco de Investigación de la UE (que asciende a 3,6 millardos de euros para un periodo de cuatro años) que cuenta con un presupuesto de 30 millones de euros para la investigación conjunta en materia de tecnologías relacionadas con la seguridad para 2001-2002.

La investigación a nivel técnico sobre criptografía se encuentra muy avanzada en Europa. El algoritmo belga conocido como "Rijndael" ganó el concurso de normas avanzadas de encripción organizado por el Instituto de normalización de los EE.UU. (NIST). El proyecto NESSIE (Nuevos esquemas europeos de firma, integridad y encripción) en el campo de las TSI ha puesto en marcha un concurso ampliado sobre algoritmos de encripción que den respuesta a los requisitos de nuevas aplicaciones multimedios, comercio móvil y tarjetas inteligentes.

Acciones propuestas:

- La Comisión propone la inclusión de la seguridad en el futuro 6º programa marco, actualmente en debate en el Consejo y el Parlamento. Para que este gasto sea óptimo, deberá vincularse con una estrategia más amplia de mejora de la seguridad de la red y de la información. La investigación financiada a través de dicho programa deberá centrarse en los retos en materia de seguridad que plantee el mundo "íntegramente digital" y en la necesidad de garantizar los derechos de los individuos y de las comunidades. Se centrará en mecanismos de seguridad básicos y su interoperabilidad, procesos dinámicos de seguridad, criptografía avanzada, tecnologías de mejora de la privacidad, tecnologías de manipulación de activos digitales y tecnologías de seguridad de funcionamiento de apoyo a funciones empresariales y organizativas en sistemas dinámicos y móviles.

- Los Estados miembros deberán fomentar activamente el uso de productos de encripción potentes y þluggable'[15] . Las soluciones en materia de seguridad basadas en la "encripción enchufable" deberán constituir una alternativa a las incluidas en los sistemas operativos.

3.5. Apoyo a la normalización y certificación orientadas al mercado

Para que las soluciones de mejora de la seguridad sean eficaces deben ser adoptadas por un conjunto significativo de agentes del mercado y basarse preferentemente en normas internacionales abiertas. Uno de los principales obstáculos para la utilización de muchas soluciones de seguridad, como por ejemplo la firma electrónica, ha sido la falta de interoperabilidad entre las distintas aplicaciones. Si dos usuarios quieren comunicarse de forma segura a través de distintos entornos debe garantizarse la interoperabilidad. Deberá fomentarse el uso de protocolos e interfaces normalizados, incluida la aplicación de pruebas de conformidad y de "interoperabilidad". Unas normas abiertas, basadas preferentemente en programas de fuentes abierta pueden contribuir a una reparación más rápida de los fallos y a una mayor transparencia.

Del mismo modo, la evaluación de la seguridad de la información contribuye a fomentar la confianza de los usuarios. El uso de criterios comunes ha facilitado el reconocimiento mutuo como método de evaluación en muchos países[16] y dichos países también han alcanzado un acuerdo con EE.UU. y Canadá para el reconocimiento mutuo de certificados de seguridad IT.

La certificación de procesos comerciales y los sistemas de gestión de la seguridad de la información reciben el apoyo de la cooperación europea para la acreditación (EA)[17]. La acreditación de organismos de certificación aumenta la confianza en su competencia e imparcialidad, fomentando así la aceptación de sus certificados en el mercado interno.

Además de la certificación, deberán llevarse a cabo pruebas de interoperabilidad. Un ejemplo de este enfoque lo constituye la Iniciativa europea para la normalización de firmas electrónicas (EESSI), que está desarrollando soluciones consensuadas en respuesta a la Directiva de la UE sobre firmas electrónicas. Otros ejemplos los constituyen la iniciativa sobre tarjetas inteligentes del programa *e*Europa y la relativa a la infraestructura de clave pública (PKI) lanzada en el marco del programa IDA de intercambio de datos entre administraciones.

No hay una falta de esfuerzo de normalización sino un gran número de normas y especificaciones distintas que conducen a la fragmentación del mercado y a la incompatibilidad de las distintas soluciones. Por lo tanto, las actividades de normalización y de certificación actuales requieren una mejor coordinación con el fin de estar al día sobre las nuevas soluciones en materia de seguridad. La armonización de especificaciones favorecerá una mayor interoperabilidad y permitirá la rápida ejecución por parte de los agentes del mercado.

Acciones propuestas:

- Se invita a Las organizaciones de normalización europeas a acelerar el trabajo sobre productos y servicios interoperables y seguros en un plazo de tiempo ambicioso y fijo. Cuando sea necesario, se seguirán nuevas formas de productos y procedimientos con el fin de acelerar el trabajo y reforzar la cooperación con los representantes de los consumidores y el compromiso de los agentes del mercado.

---

[15] Þluggable' significa que un programa informático de encripción puede instalarse fácilmente y funcionar perfectamente en sistemas operativos.

[16] Recomendación del Consejo 95/144/CE sobre criterios comunes de evaluación de las seguridad de la tecnología de la información (aplicado por la mayor parte de los Estados miembros de la UE).

[17] Cooperación europea en materia de acreditación entre 25 organismos de acreditación de la UE, AELC, y países candidatos.

- La Comisión seguirá apoyando, principalmente a través de los programas TSI e IDA, el uso de las firmas electrónicas, la aplicación de soluciones de infraestructuras de clave pública de fácil uso e interoperables y la extensión del uso de los protocolos IPv6 e IPSec [18](como se dispone en el plan de acción *e*Europa 2002).

- Se invita a los Estados miembros a que fomenten el uso de procedimientos de certificación y de acreditación de normas europeas e internacionales generalmente aceptadas que favorezcan el reconocimiento mutuo de certificados. La Comisión evaluará la necesidad de adoptar una iniciativa legal sobre el reconocimiento mutuo de los certificados antes de finales de 2001.

- Se incita a los agentes del mercado a que participen de forma más activa en las actividades de normalización europeas (CEN, Cenelec, ETSI) e internacionales (Internet Engineering Task Force (IETF) , World Wide Web Consortium (W3C)).

- Los Estados miembros deberían revisar todos las normas de seguridad pertinentes. Se podrían organizar concursos en cooperación con la Comisión para encontrar soluciones en materia de seguridad de cara a favorecer las normas acordadas a nivel internacional.

3.6. Marco Legal

Existen varios textos legales que afectan a la seguridad en las redes de comunicación y en los sistemas de información, de los que el marco reglamentario para las telecomunicaciones es el más exhaustivo. Dada la convergencia de las redes, en los temas de seguridad confluyen ahora reglamentaciones y tradiciones reguladoras procedentes de varios sectores. Entre éstos figuran las telecomunicaciones (que incluyen todas las redes de comunicación) que está siendo regulado y desregulado al mismo tiempo, el sector de la industria informática, ampliamente desregulada19, Internet que ha funcionado de forma muy libre y el comercio electrónico qué está cada vez más sujeto a una regulación específica. Por lo que se refiere a la seguridad conviene mencionar las disposiciones en materia de responsabilidad civil, ciberdelincuencia, firmas electrónicas, protección de datos y reglamentación de la exportación. De entre ellas, son de especial importancia varias disposiciones como las directivas de protección de datos, el marco reglamentario para las telecomunicaciones, y varias iniciativas legales en el contexto de la Comunicación sobre la ciberdelincuencia.

La protección de la privacidad es un objetivo político clave de la Unión Europea. El artículo 8 del Convenio europeo de Derechos Humanos lo reconoce como un derecho fundamental[20]. Los artículos 7 y 8 de la Carta de Derechos fundamentales de la Unión Europea[21] también establece el derecho al respeto de la vida familiar y privada, el hogar y las comunicaciones y los datos personales.

Las Directivas sobre protección de datos[22] y en concreto el artículo 5 de la Directiva sobre protección de datos de las telecomunicaciones[23] obligan a los Estados miembros a garantizar la

---

[18] IPv6 es un protocolo de Internet que aumenta el número de direcciones IP posibles, optimizando el encaminamiento de mensajes y mejorando las posibilidades de desplegar IPSec. IPSec es otro protocolo de Inernet cuyo fin es ofrecer confidencialidad, garantizar que los paquetes solo los ve el receptor y suministrar autenticación e integridad para garantizar que los datos del paquete son auténticos y proceden del remitente correcto..

[19] Se trata de requisitos de seguridad que afectan a los componentes eléctricos de un ordenador, pero no de requisitos de seguridad de los datos manejados en el ordenador.

[20] http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

[21] DO C 364 de 18.12.2000, www.ue.eu.int/df/docs/en/CarteEN.pdf

[22] Directivas 95/46/CE (DO L281 de 23.11.1995) y 97/66/CE (DO L24 de 30.1.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

confidencialidad en las redes públicas de telecomunicaciones y en los servicios de telecomunicaciones públicos. Además, y con el fin de aplicar el artículo 5, de acuerdo con el artículo 4 de la misma Directiva, los proveedores de servicios públicos y redes deberán adoptar las medidas técnicas y organizativas adecuadas para salvaguardar la seguridad de sus servicios. De acuerdo con dicho artículo, dichas medidas deberán garantizar un nivel de seguridad adecuado al riesgo que se presente y en consonancia con la evolución de la técnica y el coste de su aplicación. Esto significa que todos los operadores de redes tienen una obligación legal de proteger las comunicaciones contra la interceptación ilegal. El carácter paneuropeo de los servicios y una mayor competencia internacional traerán consigo una mayor armonización de estas disposiciones.

La Directiva 95/46/CE sobre protección de los datos, estipula en su artículo 17 que los controladores y los responsables del tratamiento deberán adoptar medidas para garantizar un nivel de seguridad adecuado para los riesgos que presente el procesamiento y la naturaleza de los datos a proteger, en particular cuando el procesamiento implica la transmisión de datos a través de una red. Deberán llevar a cabo medidas técnicas y organizativas para evitar la destrucción accidental o ilícita, pérdida accidental, alteración, difusión o acceso no autorizado, en particular cuando el tratamiento implica la transmisión de datos a través de una red, y contra cualquier otra forma de tratamiento ilícita. Estas disposiciones tienen implicaciones para los requisitos de seguridad en las redes y sistemas de información utilizados por las personas y organizaciones a las que hacen referencia, por ejemplo, a los proveedores de servicios de comercio electrónico. El carácter paneuropeo de los servicios y una mayor competencia transfronteriza traerán una mayor necesidad de especificación de los medios necesarios para cumplir las disposiciones mencionadas.

El **marco de la UE para los servicios de telecomunicaciones** contiene varias disposiciones por lo que se refiere a la "seguridad de funcionamiento de las redes" (es decir, disponibilidad de las redes en caso de emergencia)[24]. La Comisión propuso un nuevo marco reglamentario para los servicios de comunicación electrónica en julio de 2000 (sometido al proceso de codecisión y, por lo tanto, a debate en el Parlamento Europeo y el Consejo). Las propuestas de la Comisión recogen, aunque con algunas modificaciones, las disposiciones existentes por lo que se refiere a la seguridad e integridad de las redes.

El marco legal existente, por lo tanto, además de cubrir los temas específicos a que hace referencia cada texto legal, abarca también algunos aspectos de las redes y los sistemas de información a los que se refiere la presente comunicación.

La **Comunicación sobre ciberdelincuencia** ha planteado el debate en la UE sobre el modo de reaccionar contra las actividades delictivas que utilizan los ordenadores y las redes electrónicas. Las discusiones seguirán desarrollándose entre todas las partes afectadas en el marco del Foro de la UE que se creará en breve, tal y como se anunciaba en la Comunicación de la Comisión sobre ciberdelincuencia. El Derecho penal de los Estados miembros debería cubrir el acceso no autorizado a redes de ordenadores y la violación de la seguridad de los datos personales. En la actualidad, no hay aproximación del Derecho penal a escala de la Unión Europea en este área. Ello puede plantear obstáculos a las investigaciones contra este tipo de delitos y no constituye un factor de disuasión fuerte para quien tenga intención de cometer algún delito en este ámbito. La aproximación de las legislaciones nacionales en materia de Derecho penal contra la intrusión en

---

[23] "Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intercepción o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente, de conformidad con el apartado 1 del artículo 14".

[24] Directiva Liberalización 90/388/CE, Directiva Interconexión 97/33/CE, Directiva Voz de telefonía 98/10/CE.

las redes de ordenadores es también importante para facilitar la cooperación judicial entre los Estados miembros.

La legítima preocupación que suscita la ciberdelincuencia requiere una investigación eficaz sobre la aplicación de la ley. No obstante, estas preocupaciones legales no deberían crear soluciones que hagan que los requisitos legales debiliten la seguridad de las comunicaciones y de los sistemas de información.

Acciones propuestas:

- Es preciso alcanzar una comprensión común de las implicaciones legales de la seguridad en las comunicaciones electrónicas. A este fin, la Comisión elaborará un inventario de las medidas nacionales que se han adoptado con arreglo al correspondiente Derecho comunitario.
- Los Estados miembros y la Comisión deberán continuar apoyando la libre circulación de los productos y servicios de encripción a través de una armonización más estrecha de los procedimientos administrativos para la exportación y una mayor distensión de los controles a la exportación.
- La Comisión propondrá una medida legislativa con arreglo al Título VI del Tratado de la Unión Europea para aproximar las leyes nacionales contra los ataques a sistemas informáticos, incluídos la piratería y los ataques de denegación de servicio.

3.7. La seguridad y la administración pública

El plan de acción *e*Europa 2002 tiene como fin fomentar una interacción más efectiva y eficaz entre los ciudadanos y la administración pública. Dado que mucha de la información intercambiada entre los ciudadanos y las administraciones es de carácter personal o confidencial (médica, financiera, legal, etc.), la seguridad es vital para garantizar una utilización eficaz. Además, el desarrollo de la administración electrónica hace de las administraciones públicas **ejemplos potenciales de soluciones seguras en materia de seguridad** y agentes del mercado con la **posibilidad de influir en la oferta a través de sus decisiones de contratación pública.**

Las administraciones públicas no deben tan solo prever requisitos de seguridad para la tecnología de los sistemas de información y comunicación, sino también desarrollar una cultura de seguridad en el seno de la organización. Ello se puede conseguir a través del establecimiento de "políticas de seguridad de la organización" hechas a medida para la institución de que se trate.

Acciones propuestas:

- Los Estados miembros deberían incorporar soluciones eficaces e interoperables en materia de seguridad de la información como requisito básico para sus actividades en el campo de la administración y contratación pública electrónicas.
- Los Estados miembros deberían introducir las firmas electrónicas en la oferta de servicios públicos en línea.
- Por lo que se refiere a la e-Comisión, la Comisión adoptará una serie de medidas para fortalecer los requisitos en materia de seguridad en sus sistemas de información y comunicación.

3.8. Cooperación internacional

Del mismo modo que las comunicaciones a través de la red cruzan las fronteras en una fracción de segundo, lo hacen los problemas de seguridad asociados a ellas. La red es tan fuerte como el

más débil de sus eslabones y Europa no puede aislarse del resto de la red mundial. Por lo tanto, la seguridad exige la cooperación internacional.

La Comisión Europea ya contribuye al trabajo de foros internacionales como los del G8, la OCDE y ONU. El sector privado también está abordando los temas de seguridad en sus propias organizaciones como la del Diálogo empresarial mundial (www.GBDe.org) o la del Proyecto Internet mundial (www.GIP.org). El diálogo continuo entre estas organizaciones será fundamental para la seguridad mundial.

Acción propuesta:

- La Comisión reforzará el diálogo con las organizaciones internacionales y socios en materia de seguridad de las redes, y en particular sobre el aumento de la seguridad de funcionamiento en las redes electrónicas.

4. Próximos pasos

La presente Comunicación ofrece el marco estratégico para la acción en este área. Se trata de un primer paso y no de un plan de acción definitivo en materia de seguridad en las redes en Europa. No obstante, ya se recogen algunas sugerencias de actuación con el fin de esbozar un marco para un enfoque común europeo. La próxima fase será la discusión del marco y de las acciones propuestas en los Estados miembros y en el Parlamento Europeo. El Consejo Europeo de Gotemburgo de los días 15 y 16 de junio podría ofrecer algunas orientaciones de cara al futuro.

La Comisión propone lanzar un amplio debate con la industria, los usuarios y las autoridades responsables de la protección de datos sobre los detalles prácticos de la aplicación de las acciones propuestas. Los comentarios pueden enviarse a eeurope@cec.eu.int hasta finales de agosto de 2001. Por lo tanto, la presente comunicación constituye una invitación a que las partes interesadas presenten sus comentarios de cara al establecimiento de un conjunto final de acciones. Este conjunto podría adoptar la forma de una mapa de carreteras a desarrollar para finales de 2001.

***